(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10078988 A**

(43) Date of publication of application: **24 . 03 . 98**

(51) Int. Cl **G06F 17/60**
G09C 1/00
H04L 9/08
H04L 9/32

(21) Application number: **09016311**

(22) Date of filing: **30 . 01 . 97**

(30) Priority: **21 . 02 . 96 JP 08 70834**
10 . 07 . 96 JP 08212933

(71) Applicant: **CARD KOOLE SERVICE KK**

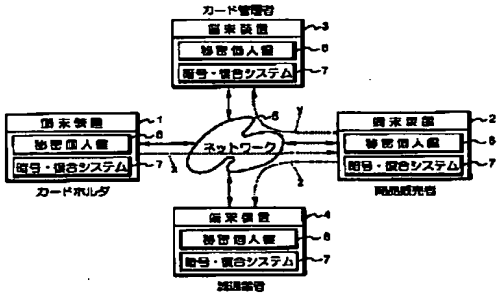
(72) Inventor: **BABA YOSHIMI**

(54) **ELECTRONIC BUSINESS TRANSACTION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a simple and versatile electronic business transaction system which eliminates the danger caused by the pretense of a commodity seller, etc., and also secures the safety for business transactions in an on-line communication mode where the credit cards are used.

SOLUTION: When a card holder purchases the commodities from a commodity seller, the card holder ciphers the partial data on the relevant commodity seller, card manager and distribution dealer among the order data necessary for purchase of commodities via his terminal equipment 1 and by means of a common cipher key effective only among those persons concerned. Then the card holder communicates with the terminal equipments 3 and 4 of the persons concerned for those ciphered data via a terminal equipment 2 of the commodity seller. Then each person concerned decodes every relevant partial data by means of the cipher key that is used in common to the card holder and carries out the desired business transaction processing.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－78988

(43)公開日　平成10年(1998)３月24日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　17/60			Ｇ０６Ｆ　15/21	３４０Ａ	
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｆ	
		7259－5Ｊ		６６０Ｂ	
Ｈ０４Ｌ　9/08			Ｇ０６Ｆ　15/21	Ｚ	
9/32				３３０	

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平9－16311

(22)出願日　平成９年(1997)１月30日

(31)優先権主張番号　特願平8－70834

(32)優先日　平８(1996)２月21日

(33)優先権主張国　日本（ＪＰ）

(31)優先権主張番号　特願平8－212933

(32)優先日　平８(1996)７月10日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　595095135
カード・コール・サービス株式会社
東京都渋谷区道玄坂１丁目22番７号

(72)発明者　馬場　芳美
千葉県船橋市宮本８丁目10番３号

(74)代理人　弁理士　佐藤　辰彦　（外１名）

(54)【発明の名称】　電子商取引システム

(57)【要約】

【課題】代金支払用のカードを利用したオンライン通信による電子商取引システムにおいて、商品販売者への成り済まし等による危険性を排除して商取引の安全性を確保しつつ、簡易で汎用性のある電子商取引システムを提供する。

【解決手段】カードを所持するカードホルダが商品販売者から商品を購入する際、その購入のための注文データのうち、商品販売者、カード管理者及び流通業者の各当事者に係わる部分データを、カードホルダの端末装置１により、それぞれの当事者との間でのみ有効な共通暗号鍵により暗号化し、それらを商品販売者の端末装置２を経由して、各当事者の端末装置２～３に通信する。各当事者はカードホルダとの共通暗号鍵を用いてそれぞれに係わる部分データを復号化して所要の商取引処理を行う。

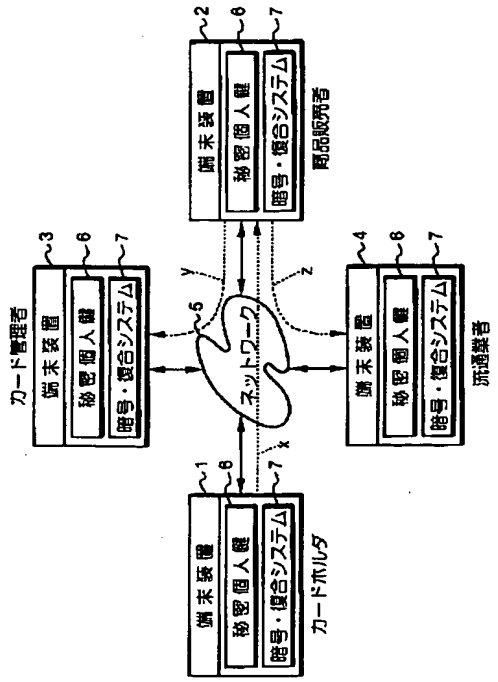


FIG. 1

【特許請求の範囲】
【請求項１】少なくとも商品販売者と、該商品販売者から代金支払用のカードを使用して商品を購入するカードホルダと、該カードによる代金支払を管理するカード管理者とを当事者として、各当事者が所持する端末装置を含むネットワークにおけるオンライン通信により商取引を行うシステムであって、
前記カードホルダが前記商品販売者から前記カードを使用して商品を購入する際、該カードホルダは自身の端末装置により、前記商品を購入するための注文データのうち、該カードホルダ以外の各当事者に係わる部分をそれぞれ該当事者との間でのみ有効な共通暗号鍵により暗号化した後、それらの暗号化したデータを一括してなる暗号化注文データを該カードホルダの端末装置から前記商品販売者の端末装置を経由して該カードホルダ以外の各当事者に通信し、
該暗号化注文データを受信した各当事者は、それぞれの端末装置により、前記暗号化注文データから前記カードホルダとの前記共通暗号鍵を用いて自身に係わる部分データのみを復号化し、
その復号化を行う当事者のうち、前記カード管理者は、自身の端末装置により復号化した部分データに基づき、前記商品販売者に前記カードホルダの認証を与える処理を含めて該カード管理者に係わる商取引の処理を行い、
前記商品販売者は、自身の端末装置により復号した部分データと前記カード管理者から与えられた前記カードホルダの認証とに基づき、前記商品を配送するための処理を含めて該商品販売者に係わる商取引の処理を行うことを特徴とする電子商取引システム。
【請求項２】前記注文データは前記商品の配送先を含むと共に、前記当事者は前記商品の配送を行う流通業者を含み、
前記注文データのうち、前記配送先のデータは前記カードホルダ及び前記流通業者間の前記共通暗号鍵のみにより暗号化され、
該流通業者は、自身の端末装置により復号した前記配送先のデータを含む前記部分データと前記商品販売者から与えられる指示とに基づき前記商品の配送処理を行うことを特徴とする請求項１記載の電子商取引システム。
【請求項３】前記注文データは、前記カードの番号及び有効期限を含み、該番号及び有効期限のデータは、前記カードホルダ及びカード管理者間の前記共通暗号鍵のみにより暗号化したことを特徴とする請求項１又は２記載の電子商取引システム。
【請求項４】前記カードホルダと該カードホルダ以外の各当事者との間の前記共通暗号鍵は、前記カードホルダ側では、該カードホルダがあらかじめ備えた該カードホルダに固有の秘密個人鍵に、該カードホルダ以外の各当事者に固有で且つ公開性の識別子を作用させて生成し、該カードホルダ以外の各当事者側では、該当事者があらかじめ備えた該当事者に固有の秘密個人鍵に、前記カードホルダに固有で且つ公開性の識別子を作用させて生成することを特徴とする請求項１乃至３のいずれかに記載の電子商取引システム。
【請求項５】前記各当事者は、前記暗号化注文データの通信を行う前に、該暗号化注文データの通信相手側とあらかじめ相互に通信を行ってその通信相手側の当事者を確認しておくことを特徴とする請求項１乃至４のいずれかに記載の電子商取引システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネット、パソコン通信等を使用してオンライン通信による商取引を行う電子商取引システムに関し、詳しくはクレジットカード、デビットカード等の代金支払用のカードを用いた電子商取引システムに関する。
【０００２】
【従来の技術】近年、インターネット、パソコン通信等の普及に伴い、それらのネットワークの利用者が、インターネット上の電子モールやパソコン通信における商店等の商品販売者に対して、オンライン通信で所望の商品の注文を行い、該商品の購入を行うことが通常的に行われるようになってきている。
【０００３】このような商取引では、商品を購入しようとする者は、クレジットカード、デビットカード等の代金支払用のカードをあらかじめ所持し、商品を購入するに際しては、その購入者であるカードホルダの氏名、住所、電話番号や購入しようとする商品の種類、個数等のデータと共に、該カードホルダのカードの番号や有効期限等のデータを該カードホルダの端末装置からネットワークを介して商品販売者に通信する。そして、商品販売者は、自身の端末装置で受信した上記のデータに基づき、カードの管理者（カード会社）からカードホルダの認証を受けたり、商品配送の手続き（流通業者に商品の配送を依頼する場合を含む）やカード会社への商品代金の請求等の処理を行う。また、カード会社は、商品販売者から与えられるカードホルダの氏名、住所、電話番号、カードの番号や有効期限等に基づきカードホルダの認証を商品販売者に与えたり、さらに商品販売者から与えられる商品代金等のデータに基づきカードホルダの口座からの商品代金の引き落とし（商品代金の決済）等の処理を行う。
【０００４】このような電子商取引システムでは、ハッキング（通信データの傍受）、クラッキング（通信データの改ざん）、あるいはカードホルダ、マーチャントサーバ（商品販売者の端末装置）、アクワイアラーゲートウェイ（カード管理者の端末装置）の成り済まし等の危険性が従来より指摘されていた。
【０００５】この場合、例えばカードホルダの成り済ましについては、カード管理者が保有し管理するカード番

号等に基づくデータベースによって、かなりな程度に防止することが可能である。また、通常、一人のカードホルダのカードによる決済金額は、その上限が設定されているため、カードホルダの成り済ましによる被害はさほど大きな金額にはならない。

【０００６】これに対して、特に商品販売者の成り済ましでは、その贋の商品販売者により多数のカード番号、有効期限等のカード情報が収集されてしまう虞れがあるため、それらのカード情報を盗用することで、多大な被害を生じる虞れがある。

【０００７】これらの問題に対する対策としては、従来、カードホルダの識別番号（ＩＤ番号）やパスワード、もしくはこれらに相当するデータを使用した通信を行い、また、該識別番号やパスワードが盗用された場合でも、カードによる既存の商取引には影響を与えないように、所謂クローズドユーザーグループ（closed user group ）を構築することが一般的に行われている。しかるに、このようなシステムでは、前述のような問題を解決することは困難なものとなっていた。

【０００８】また、ＤＥＳ等を用いたストリーム型共通鍵暗号による通信データの暗号化や、ＲＳＡ暗号等の公開鍵暗号による認証等、前述のような個々の問題に対する対策手法は種々提案されているが、電子商取引システムとして簡易で汎用性のあるシステムは未だ構築されていないのが実情である。

【０００９】

【発明が解決しようとする課題】本発明はかかる背景に鑑み、代金支払用のカードを利用したオンライン通信による電子商取引システムにおいて、商品販売者への成り済まし等による危険性を排除して商取引の安全性を確保しつつ、簡易で汎用性のある電子商取引システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明の電子商取引システムはかかる目的を達成するために、少なくとも商品販売者と、該商品販売者から代金支払用のカードを使用して商品を購入するカードホルダと、該カードによる代金支払を管理するカード管理者とを当事者として、各当事者が所持する端末装置を含むネットワークにおけるオンライン通信により商取引を行うシステムであって、前記カードホルダが前記商品販売者から前記カードを使用して商品を購入する際、該カードホルダは自身の端末装置により、前記商品を購入するための注文データのうち、該カードホルダ以外の各当事者に係わる部分をそれぞれ該当事者との間でのみ有効な共通暗号鍵により暗号化した後、それらの暗号化したデータを一括してなる暗号化注文データを該カードホルダの端末装置から前記商品販売者の端末装置を経由して該カードホルダ以外の各当事者に通信し、該暗号化注文データを受信した各当事者は、それぞれの端末装置により、前記暗号化注文データから前記カードホルダとの前記共通暗号鍵を用いて自身に係わる部分データのみを復号化し、その復号化を行う当事者のうち、前記カード管理者は、自身の端末装置により復号化した部分データに基づき、前記商品販売者に前記カードホルダの認証を与える処理を含めて該カード管理者に係わる商取引の処理を行い、前記商品販売者は、自身の端末装置により復号した部分データと前記カード管理者から与えられた前記カードホルダの認証とに基づき、前記商品を配送するための処理を含めて該商品販売者に係わる商取引の処理を行うことを特徴とする。

【００１１】かかる本発明によれば、前記商品販売者から代金支払用のカードを使用して商品を購入しようとするカードホルダは、前記注文データのうち、前記商品販売者やカード管理者等、該カードホルダ以外の各当事者が係わる部分のデータを各当事者との間でのみ有効な共通暗号鍵により暗号化した上で、それらの暗号化したデータを復号してなる暗号化注文データを、該カードホルダの端末装置から商品販売者の端末装置を経由して該商品販売者を含む各当事者に通信する。このように注文データを暗号化することで、その機密性が保たれる。

【００１２】一方、この暗号化注文データを受け取った商品販売者、カード管理者等の各当事者は、該暗号化注文データから、該当事者に係わる部分データを前記カードホルダとの間の共通暗号鍵によって復号化する。この場合、各当事者は、他の当事者のみに係わる部分データについては、それを復号化するための共通暗号鍵を有しないため、該部分データを復号化してその内容を知ることはできず、換言すれば該当事者が関与する範囲内でしか、前記注文データの内容を知ることができない。従って、該当事者が関与しない部分データを盗用することはできない。そして、前記当事者のうち、カード管理者は復号化した部分データに基づき、前記商品販売者に前記カードホルダの認証を与える処理を含めて該カード管理者に係わる商取引の処理を行い、前記商品販売者は、自身の端末装置により復号した部分データと前記カード管理者から与えられた前記カードホルダの認証とに基づき、前記商品を前記カードホルダに受け渡すための処理を含めて該商品販売者に係わる商取引の処理を行う。これにより、電子商取引が成立する。

【００１３】従って、本発明によれば、注文データを暗号化して通信することで、その機密性が確保されると同時に、前記カードホルダ以外の各当事者には、前記注文データのうち、必要最小限のデータしか与えられないこととなる。このため第三者が仮に商品販売者に成り済ましても、その贋の商品販売者は、例えばカードの番号や有効期限等、カード管理者のみに係わる情報を取得することができず、商品販売者への成り済ましによる実効が得られない。これにより本発明によれば、商品販売者への成り済まし等の危険性を排除しつつ商取引の安全性を確保することができる。また、前記カードホルダの端末

装置で生成した暗号化注文データは、商品販売者を経由して各当事者に配付されるので、カードホルダは、商品の購入に際しては、前記暗号化注文データを実質的には商品販売者のみに通信すればよく、簡素な電子商取引システムを実現することができる。

【００１４】かかる本発明の電子商取引システムでは、前記注文データに前記商品の配送先（これは前記カードホルダの所在地とは限らない）が含まれ、また、前記当事者として商品の配送を行う流通業者が含まれる場合もある。

【００１５】そして、この場合には、前記注文データのうち、前記配送先のデータは前記カードホルダ及び前記流通業者間の前記共通暗号鍵のみにより暗号化され、該流通業者は、自身の端末装置により復号した前記配送先のデータを含む前記部分データと前記商品販売者から与えられる指示とに基づき前記商品の配送処理を行うことが好ましい。このようにすることで、商品の配送先は、前記当事者のうち、前記流通業者のみが知り得るものとなり、プライバシーの保護の点で好ましい。

【００１６】また、本発明では、前記注文データは、前記カードの番号及び有効期限を含み、該番号及び有効期限のデータは、前記カードホルダ及びカード管理者間の前記共通暗号鍵のみにより暗号化する。これにより、前記代金支払用のカードを使用して商取引を行う際に決済上、最も重要なカードの番号及び有効期限は、そのデータを必要とする前記カード管理者のみが前記暗号化注文データを復号化して知ることができ、逆に言えば、該カード管理者及びカードホルダ以外の当事者はカードの番号及び有効期限のデータを知ることができないこととなる。これにより、前述の電子商取引システムの安全性を効果的に確保することができると共に、その商取引上、最も危険性の高い商品販売者への成り済ましを効果的に防止することができる。

【００１７】以上のような本発明では、前記共通暗号鍵は、前記カードホルダと各当事者との間で別途あらかじめ取り決めて配付しておく等してもよいが、前記カードホルダと該カードホルダ以外の各当事者との間の前記共通暗号鍵は、前記カードホルダ側では、該カードホルダがあらかじめ備えた該カードホルダに固有の秘密個人鍵に、該カードホルダ以外の各当事者に固有で且つ公開性の識別子を作用させて生成し、該カードホルダ以外の各当事者側では、該当事者があらかじめ備えた該当事者に固有の秘密個人鍵に、前記カードホルダに固有で且つ公開性の識別子を作用させて生成することが特に好ましい。ここで、前記識別子は、各当事者の氏名、名称、住所、ネットワーク上のメールアドレス、ドメイン名、あるいはそれらを組み合わせたもの等、各当事者に対して固定的に用いられ、且つ公開性のあるものであればよい。

【００１８】このように、カードホルダを含めた各当事者が、自己の前記秘密個人鍵に共通暗号鍵を共有すべき相手側の識別子を作用させて共通暗号鍵を生成する方式を採用することで、各当事者は、自己の秘密個人鍵に相手側の識別子を入力するだけで、事前に共通暗号鍵の取り決めや配付等を行うことなく前述の商取引に必要な共通暗号鍵を生成することができる。このため、本発明の電子商取引システムを極めて簡素なものとすることができると共に、その汎用性を高めることができる。さらに共通暗号鍵自体の事前配付が必要ないため、通信データの機密性を確実に確保することができ、電子商取引システムの安全性を高めることができる。

【００１９】尚、上記のような共通暗号鍵の生成方式は、例えばRolf Blom による論文「NON-PUBLIC KEY DISTRIBUTION ／Advances in Cryptology:Proceedings of CRYPTO'82／Plenum Press 1983, pp. 231-236」、同じくRolf Blom による論文「An Optimal Class of Symmetric Key Generation Systems／Advances in Cryptology:EUROCRYPT '84 ／Springer LNCS 209, 1985, pp. 335-338」、あるいは特公平５－４８９８０号公報等に開示されているので、ここでは詳細な説明を省略する。

【００２０】さらに、本発明では、前記各当事者は、前記暗号化注文データの通信を行う前に、該暗号化注文データの通信相手側とあらかじめ相互に通信を行ってその通信相手側の当事者を確認しておくことが好ましい。このように電子商取引に関与する当事者の事前確認を行っておくことで、商品販売者やカード管理者等への成り済ましによる弊害を事前に予防することができ、電子商取引システムの安全性をより一層高めることができる。

【００２１】

【発明の実施の形態】本発明の一実施形態を図１及び図２を参照して説明する。

【００２２】図１を参照して、本実施形態の電子商取引システムでは、クレジットカード、デビットカード等の代金支払用のカード（図示せず）を所持するカードホルダの端末装置１と、商品販売者の端末装置２と、カードによる代金支払を管理するカード管理者（カード会社）の端末装置３と、商品販売者が扱う商品の配送業務を担う流通業者の端末装置４とがインターネット、パソコン通信網等のネットワーク５を介して相互に通信可能に接続されている。そして、これらのカードホルダ、商品販売者、カード管理者及び流通業者を後述の電子商取引を行う当事者としている。

【００２３】各当事者の端末装置１～４は、パソコン等のコンピュータマシンにより構成されたものである。そして、それらの各端末装置１～４には、任意の当事者間で暗号通信用の共通暗号鍵を生成するための共通暗号鍵生成用システムである秘密個人鍵６と、その共通暗号鍵による通信データの暗号化・復号化を行うための暗号・復号システム７とがソフトウェアもしくはハードウェアとして含まれ、これらのシステム６，７は暗号鍵の発行

等を行う図示しないセンターから各当事者に事前に配付されている。

【００２４】ここで、上記秘密個人鍵６は、前述のRolf Blom による論文や特公平５－４８９８０号公報等に見られるように、各当事者に固有のもので、通信相手側の氏名、住所等、各当事者に固有でしかも公開性の識別子を各端末装置１～４により入力することで、その通信相手側との共通暗号鍵を生成するものである。

【００２５】また、前記暗号・復号システム７は、周知のＤＥＳ（Data Encryption Standard）等を用いて前記共通暗号鍵により通信データを暗号化したり（通信データの送信側）、その暗号化された通信データを復号化する（通信データの受信側）ものである。

【００２６】以上のような構成を具備する本実施形態の電子商取引システムでは、次のように電子商取引が行われる。

【００２７】まず、本実施形態のシステムでは、各当事者は、インターネットやパソコン通信等を通じて随時、後述の暗号化注文データの通信を行うべき相手側と各端末装置１～４を介して相互に通信を行っているものとし、これにより、後述の暗号化注文データの通信を行うべき当事者同士で相互に相手側が正当に存在しているか等の確認（通信相手側の認証）が事前になされている。

【００２８】また、カードホルダは、事前に、自身の端末装置１と商品販売者の端末装置２との通信（商品販売者のホームページの参照等）によって、あるいは、商品販売者のカタログデータをＣＤ－ＲＯＭ等の記録媒体もしくは雑誌等により参照しておくことによって、商品販売者の商品情報を取得している。

【００２９】そして、カードホルダが商品販売者の商品を購入しようとするとき、その旨をカードホルダから商品販売者に通知し、該商品販売者から注文書書式のデータを送付してもらう。尚、この注文書書式のデータは、カードホルダ自身があらかじめＣＤ－ＲＯＭ等から取得するようにしてもよい。

【００３０】次いで、カードホルダは、取得した注文書書式に従って自身の端末装置１により、所望の商品を自身のカードにより購入するための注文データを入力する。この場合、入力する注文データとしては、例えば図２に示すようにカードホルダの氏名、住所、電話番号、ＦＡＸ番号、カードホルダが所持するカードの番号及び有効期限、購入しようとする商品の品名、数量、商品番号、購入金額、代金の支払い形態（分割払い、一括払い等）、商品の配送先（配送先の宛て名、住所等を含む）等がある。

【００３１】尚、この注文データは、上記のデータに限られるわけではなく、カードホルダが自身のカードを使用して商品を購入する際に、その商取引の当事者となる商品販売者、カード管理者及び流通業者がそれぞれその商取引に係わる処理（商品販売者による注文者や注文内容の特定、カード管理者によるカードホルダの認証及び代金の決済、流通業者による商品の配送等）を遂行するために必要な情報が含まれていればよい。

【００３２】かかる注文データを作成した後、カードホルダは、さらに自身の端末装置１により、その注文データのうち、商品販売者、カード管理者及び流通業者の各当事者に係わる部分のデータ（これはあらかじめ定められている）をそれぞれ抽出して複製する。例えば、図２を参照して、商品販売者に関しては、前述の注文データのうち、カードホルダの氏名、住所、電話番号、ＦＡＸ番号、購入しようとする商品の品名、数量、商品番号、購入金額、代金の支払い形態等、注文者や注文内容を特定するためのデータが複製され、カード管理者に関しては、カードホルダの氏名、住所、電話番号、ＦＡＸ番号、カードホルダが所持するカードの番号及び有効期限、購入しようとする商品の商品番号、購入金額、代金の支払い形態等、カードホルダの認証や代金の決済を行うためのデータが複製される。また、流通業者に関しては、カードホルダの氏名、電話番号、ＦＡＸ番号、配送先等、商品の配送を行うために必要なデータが複製される。

【００３３】尚、このような処理をカードホルダが行うための手順、あるいはそれを自動処理するソフトウェアが、商品販売者から前記注文書書式のデータをカードホルダに送付する際等に、あらかじめ該カードホルダに与えられている。そして、カードホルダは上記の処理を与えられた手順に従って、あるいは与えられたソフトウェアにより行う。また、各当事者毎の部分データは、上記のような態様に限られるものではなく、例えば前記ＦＡＸ番号のデータはいずれの当事者でも不要の場合があり、また、各国の法律や慣習等のために、カード管理者にとって商品番号が不要であったり、商品販売者にとって商品の配送先が必要であったりする。

【００３４】さらに、カードホルダは、自身の端末装置１において、前記秘密個人鍵６に商品販売者、カード管理者及び流通業者の各当事者の前記識別子をそれぞれ各別に入力することで、それらの各当事者との間の暗号通信のための前記共通暗号鍵をそれぞれ生成する。この場合、流通業者は商品販売者が指定するものなので、該流通業者の識別子、もしくはそれをカードホルダが認識するために必要な情報（流通業者の名称等）が、例えば商品販売者から前記注文書書式のデータをカードホルダに送付する際等に、該カードホルダに事前に与えられている。尚、商品販売者及びカード管理者は、カードホルダ自身が特定したものであるので、該カードホルダは商品販売者及びカード管理者の識別子を既に認知している。

【００３５】このようにして、前記注文データから商品販売者、カード管理者及び流通業者の各当事者に係わる部分データを複製すると共に、それらの各当事者との間の共通暗号鍵を生成した後、カードホルダは、自身の端

末装置１の前記暗号・復号システム７により、図２に示すように各当事者に係わる部分データをその当事者に対応する共通暗号鍵を用いて暗号化し、さらにその暗号化した各部分データを一括してなる暗号化注文データとカードホルダの識別子とを１セットの通信データとして、自身の端末装置１からネットワーク５を介して商品販売者の端末装置２に送信する（図１の破線矢印ｘを参照）。この場合、暗号化注文データと共に送信するカードホルダの識別子は暗号化されない。尚、カードホルダの識別子の代わりに、商品販売者等の各当事者がカードホルダの識別子を特定し得る情報（カードホルダの単なる氏名、住所等）を暗号化注文データと共に送信するようにしてもよい。

【００３６】このとき、上記の通信データの主要部たる暗号化注文データは、暗号化されているため、それを当事者でない第三者が解読したりすることはできず、該通信データの機密性が確保される。

【００３７】一方、かかる通信データ（暗号化注文データ及びカードホルダの識別子）を端末装置２で受信した商品販売者は、該通信データに含まれるカードホルダの識別子を、自身の端末装置２の秘密個人鍵６に入力することで、カードホルダとの共通暗号鍵を生成する。そして、図３を参照して、商品販売者は、生成した共通暗号鍵を用いて、自身の端末装置２の前記暗号・復号システム７により前記暗号化注文データの自身に係わる部分データを復号化する。これにより、前記注文データのうちの、カードホルダの氏名、住所、電話番号、ＦＡＸ番号、購入しようとする商品の品名、数量、商品番号、購入金額、代金の支払い形態等、商品販売者にとって必要なデータが正規に得られる。

【００３８】このとき、商品販売者以外の当事者（カード管理者及び流通業者）に係わる部分データについては、商品販売者及びカードホルダ間の共通暗号鍵とは異なる暗号鍵で暗号化されているため、商品販売者はそれらの部分データを復号することはできず、従って、例えばカード管理者に係わるカードの番号や有効期限、あるいは流通業者に係わる配送先のデータの内容を知ることはできない。

【００３９】さらに商品販売者は、前記暗号化注文データ及びカードホルダの識別子を自身の端末装置２からカード管理者の端末装置３にネットワーク５を介して送信する（図１の破線矢印ｙを参照）。この場合、商品販売者が受信した全データをカード管理者に送信してもよいが、暗号化注文データのうちのカード管理者に係わる部分データのみをカードホルダの識別子と共にカード管理者に送信してもよい。

【００４０】このようにして暗号化注文データ及びカードホルダの識別子を商品販売者の端末装置２から自身の端末装置３で受信したカード管理者は、商品販売者の場合と同様に、カードホルダの識別子を、自身の端末装置３の秘密個人鍵６に入力することで、カードホルダとの共通暗号鍵を生成した後、図３に示すようにその共通暗号鍵を用いて、自身の端末装置３の前記暗号・復号システム７により前記暗号化注文データの自身に係わる部分データを復号化する。これにより、前記注文データのうちの、カードホルダの氏名、住所、電話番号、ＦＡＸ番号、カードホルダが所持するカードの番号及び有効期限、購入しようとする商品の商品番号、購入金額、代金の支払い形態等、カード管理者にとって必要なデータが正規に得られる。このとき、カード管理者は、商品販売者の場合と同様に、前記暗号化注文データのうちの、自身に係わる部分データ以外のデータ、例えば流通業者のみに係わる商品の配送先等のデータは知ることができない。

【００４１】そして、前述のデータを獲得したカード管理者は、カードホルダの氏名、電話番号、カードの番号及び有効期限等のデータに基づき、カードホルダの認証（カードホルダが適正なカード使用者であるか否か）を行い、その認証結果を商品販売者に通知する。さらに、カードホルダが適正なカード使用者であれば、購入金額、代金の支払い形態等のデータに基づき、カードホルダの口座から代金を引き落とすための処理を行う。

【００４２】また、前記認証結果の通知をカード管理者から受けた商品販売者は、その認証結果が適正であれば、前記暗号化注文データ及びカードホルダの識別子を自身の端末装置２から流通業者の端末装置４にネットワーク５を介して送信する（図１の破線矢印ｚを参照）と共に、該商品販売者が獲得した部分データに基づき商品配送の依頼を流通業者に与えたり、必要に応じて商品の仕入れ手配等を行う。この場合、暗号化注文データのうちの流通業者に係わる部分データのみをカードホルダの識別子と共に流通業者に送信してもよい。

【００４３】そして、商品販売者から暗号化注文データ及びカードホルダの識別子を受け取った流通業者は、商品販売者及びカード管理者の場合と同様に、カードホルダの識別子を、自身の端末装置４の秘密個人鍵６に入力することで、カードホルダとの共通暗号鍵を生成した後、図３に示すようにその共通暗号鍵を用いて、自身の端末装置４の前記暗号・復号システム７により前記暗号化注文データの自身に係わる部分データを復号化する。これにより、前記注文データのうちの、カードホルダの氏名、電話番号、ＦＡＸ番号、配送先等、流通業者にとって必要なデータが正規に得られる。このとき、流通業者は、商品販売者やカード管理者の場合と同様に、前記暗号化注文データのうちの、自身に係わる部分データ以外のデータ、例えばカードの番号や有効期限等のデータは知ることができない。

【００４４】尚、前述の配送先等のデータを獲得した流通業者は、そのデータと商品販売者から与えられた指示とに基づき、商品配送の処理を行う。

【００４５】以上のように構築された本実施形態の電子商取引システムでは、カードホルダが作成する注文データのうちの、各当事者（商品販売者、カード管理者及び流通業者）に係わる部分データをそれぞれ各当事者との間での各別の共通暗号鍵を用いて暗号化し、それらの暗号化した部分データを各当事者に通信により配付するようにしているため、注文データの機密性を確保することができる。同時に、各当事者は、カードホルダとの共通暗号鍵を使用することで、注文データのうちの必要なデータを支障なく獲得することができる一方、逆に言えば必要なデータのみしか獲得することができない。このため、例えば商品販売者あるいは流通業者は、カードを使用した商取引上、最も重要なカードの番号や有効期限を知ることができない。従って、仮に第三者が商品販売者や流通業者に成り済ましても、カードの番号や有効期限等の重要情報を獲得することができないために、実効が得られず、これにより、商品販売者あるいは流通業者への成り済ましを防止することができる。

【００４６】また、カードホルダを含めた各当事者は、前記暗号化注文データの通信を行う相手側と事前に通信を行って、相手側の当事者を確認しているので、商品販売者あるいは流通業者への成り済ましのみならず、カード管理者の成り済ましも予防することができる。

【００４７】尚、本願発明者等が、本実施形態の電子商取引システムによる実証実験を行って、成り済まし等による種々のシステム攻撃を加えてみたところ、充分にそれらの攻撃に耐え得るものであった。

【００４８】また、本実施形態では、商品の配送先は、流通業者とカードホルダとの間の共通暗号鍵のみにより暗号化しているため、そのデータを商品販売者やカード管理者が知ることはできず、これにより、カードホルダが購入した商品を自身とは別の人に贈る場合等に、プライバシーを保護することができる。

【００４９】さらに、カードホルダが商品を購入するに際しては、前記暗号化注文データは、商品販売者の端末装置２を経由して、該商品販売者の他、カード管理者や流通業者に配送されるため、カードホルダは商品販売者の端末装置２にのみ暗号化注文データを送信すればよく、簡単に商品の購入を行うことができる。

【００５０】また、本実施形態では商品販売者、カード管理者及び流通業者に係わる部分データをカードホルダが暗号化し、また、商品販売者、カード管理者及び流通業者がそれぞれ部分データを復号化するための共通暗号鍵は、各当事者が自身の端末装置１～４に備えた秘密個人鍵に、所要の当事者の識別子を入力するだけで生成することができるので、商取引を行う都度、当事者間で共通暗号鍵を取り決めたり、別途のセンターから共通暗号鍵を配付してもらったりする必要がなく、簡単に商取引を行うことができる。

【００５１】従って、本実施形態の電子商取引システムを安全且つ簡素で汎用性のあるシステムとすることができる。

【００５２】尚、以上説明した本実施形態では、電子商取引の当事者として流通業者を含めたシステムを示したが、該流通業者を含めずにシステムを構築してもよく、あるいは、インターネットプロバイダ等のゲートウェイ管理者や鍵認証局等を当事者として含めてシステムを構築することも可能である。

【００５３】また、本実施形態では、各当事者が自身の端末装置１～４に備えた秘密個人鍵に、所要の当事者の識別子を入力することで、共通暗号鍵を生成するシステムを示したが、当事者間で共通暗号鍵を別途取り決めたり、センターから共通暗号鍵を配付してもらったりするようにすることも可能である。

【図面の簡単な説明】

【図１】本発明の電子商取引システムの一実施形態のシステム構成図。

【図２】図１のシステムにおけるカードホルダ側でのデータ処理を示す説明図。

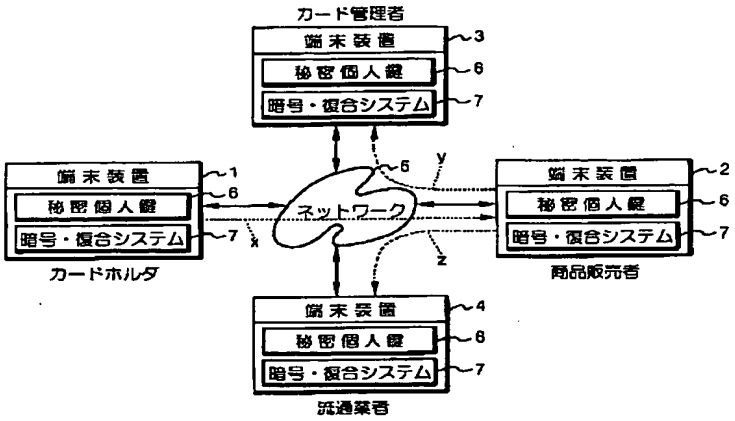
【図３】図１のシステムにおけるカードホルダ以外の当事者側でのデータ処理を示す説明図。

【符号の説明】

１～４…端末装置、５…ネットワーク、６…秘密個人鍵。

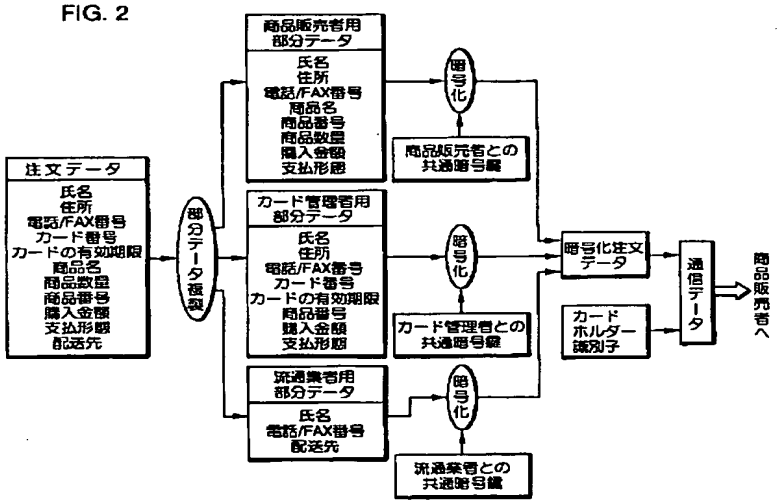
【図１】

FIG. 1



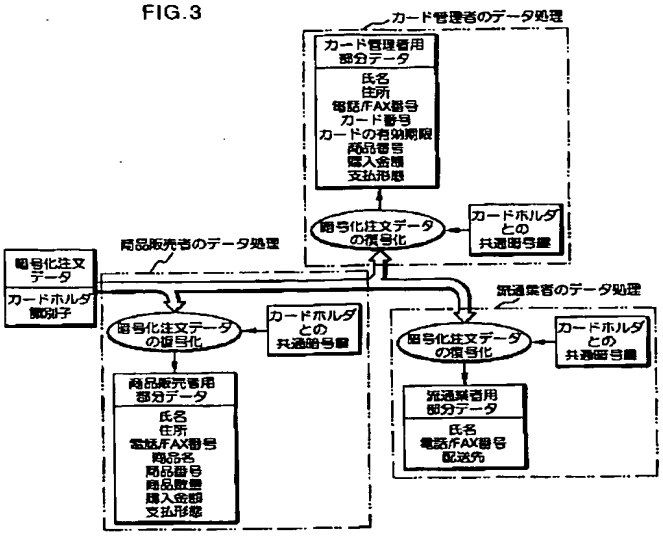
【図２】

FIG. 2



【図３】

FIG.3



フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	FI		技術表示箇所
			H04L 9/00	601E	
				675D	